Thailand National Root Certification Authority

Certification Practice Statement

Version 3.0

Certificate Practice Statement Identifier (OID): 2.16.764.1.1.1.11004.4.1

<Document Status>

- *Draft*
- *Internal Use*
- *Publication*

Document Revision History

Date	Version	Description
August 2013	1.0	Initial Release
June 2014	2.0	• Translated into English for WebTrust assessment • Reviewed contents to align with RFC 3647 • Reviewed consistency of terms in the document • Added short description of Thailand NRCA • Introduced Software Developer in topic 5.2.1 • Added topic 6.5.1 Computer Security Technical Requirements • Added topic 6.5.2 Computer Security Rating
May 2015	2.1	• Revised 1.5.2 Contact Person • Revised 2.2 Publication of Certification Information • Revised 9.13.1 Disputes between Issuer and subscriber
August 2015	3.0	• Revised 1.1 Overview • Revised 1.5.2 Contact Person • Added 1.5.5 CP Review and update Procedures • Revised 4.3.1 CA Actions during Certificate Issuance • Revised 4.9.1 Circumstances for Revocation • Revised 4.9.3 Procedure for Revocation Request • Added 5.4.9 Penetration Test Assessments • Revised 7.1.2.2 Certificate Policies Extension • Revised 8 Compliance Audit and Other Assessments • Revised 8.5 Topics Covered by Assessment

Table of Contents

1. Introduction

1.1 Overview

The Electronic Transactions Act sets out the legal framework for the public key infrastructure (PKI) with the objectives of facilitating the use of electronic transactions in a secure manner for commercial and other purposes. PKI is composed of many elements, including legal obligations, policies, hardware, software, databases, networks, personnel and operating procedures. The center of trust in PKI is Certification Authority (CA), who issues a digital certificate to a person or legal entity (who may be another CA) by using a collection of hardware, software, personnel, and operating procedures. The digital certificate will bind a public key to that person or legal entity. It allows relying parties to trust signatures or assertions made by the person or legal entity using the private key that corresponds to the public key contained in the certificate. A digital certificate when combined with private key can be used to verify the identity in electronic transactions using the Digital Signature mechanism. Any person or legal entity who wishes to use a digital certificate must pass the certification authority's authentication procedures.

In an environment where there are multiple certification authorities, certificate usage and authentication will be troublesome if the certification authorities are not in a Trust Relationship model. The basic way to solve the problem is to build a trust relationship among certification authorities, which will be unmanageable in the long run. Therefore, the Electronic Transactions Commission (ETC) has agreed to form a trust relationship in the hierarchy model for all certification authorities in Thailand.

In 2007 (B.E. 2550), the Ministry of Information and Communication Technology (MICT) has established the Thailand National Root Certification Authority or Thailand NRCA with the objective to centralize the management of trust relationship and serve as the hub of trust, so called Trust Anchor, so that certificates issued by subordinate certification authorities can seamlessly work together.

This document is the Thailand National Root Certification Authority (Thailand NRCA) Certification Practice Statement (CPS). It states the practices that Thailand NRCA employs in providing certification services, including without limitation, issuing, managing, revoking, and renewing certificates in accordance with the specific requirements of the Thailand NRCA Certificate Policy (CP).

NRCA conforms to the current version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates published at http://www.cabforum.org. In the event of any inconsistency between this document and those Requirements, those Requirements take precedence over this document.

The CP is the principal statement of policy governing the Thailand NRCA. The CP applies to all subordinate certification authorities under Thailand NRCA and thereby provides assurances of uniform trust throughout Thailand NRCA. The CP sets forth requirements that subordinate certification authorities under Thailand NRCA must meet. This CPS describes how Thailand NRCA meets these requirements. More specifically, this CPS describes the practices that Thailand NRCA employs for:

- managing and securing the core infrastructure that supports Thailand NRCA, and issuing, managing, revoking, and renewing certificates under Thailand NRCA.

Mission of Thailand NRCA includes:

- Certificate issuance, publication, and revocation for certification authorities located in Thailand; and
- Coordinate with overseas certification authorities to enable seamless international usage of certificates issued by local certification authorities.

This CPS also sets out the certification service scope and procedures of Thailand NRCA, as well as to specify duties, functions, legal obligations and potential liabilities of participants in the systems used by Thailand NRCA. The document structure and topics conform to the Internet Engineering Task Force (IETF) RFC 3647 for Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.

1.2 Document Name and Identification

This document is the Thailand National Root Certification Authority (Thailand NRCA) Certification Practice Statement (CPS). This CPS is published for public knowledge on Thailand NRCA Website.

1.3 PKI Participants

1.3.1 Certification Authority

Thailand National Root Certificate Authority (Thailand NRCA) is an operational unit operated by Electronic Transactions Development Agency (Public Organization) under the Ministry of Information and Communication Technology. Thailand NRCA issues digital certificates to a legal entity (who operates CA in Thailand) by using a collection of hardware, software, personnel, and operating procedures that create, sign, and issue public key certificates to CA subscribers. This includes centralized, automated systems such as card management systems. Thailand NRCA is responsible for issuing and managing certificates including:

- Approving the issuance of all certificates, including those issued to subordinate CAs and RAs
- Publication of certificates
- Revocation of certificates
- Generation and destruction of CA signing keys
- Establishing and maintaining Thailand NRCA system
- Establishing and maintaining the Certification Practice Statement (CPS)
- Ensuring that all aspects of the CA services, operations, and infrastructure are performed in accordance with the requirements, representations, and warranties of the CP.

1.3.2 Registration Authority

Registration Authority (RA) is a person or legal entity that collects and verifies each subscriber's identity and information that is to be entered into the subscriber's public key certificate. RA performs its function in accordance with the CPS of the CA and is responsible for:

- The registration process
- The identification and authentication process.

1.3.3 Subscribers

Subscriber is a person or legal entity whose name appears as the subject in a certificate. The Subscriber asserts the use of the key and certificate in accordance with the Certificate Policy asserted in the certificate. CAs are sometimes technically considered "subscribers" in a PKI. However, the term "Subscriber" as used in this CPS refers only to "CA Subscriber" who request certificates for signing and issuing certificates or certificate status information. CAs who want to apply for a certificate from Thailand NRCA for signing and issuing certificates or certificate status information, and so become a subordinate CA of Thailand NRCA and will be qualified as CA Subscriber.

1.3.4 Relying Parties

Relying Party is a person or entity that acts in reliance on the validity of the binding of the subscriber's name to a public key. The Relying Party uses a subscriber's certificate to verify a digital signature that is generated using the private key corresponding to the public key listed in a certificate. A Relying Party may or may not be a subscriber under Thailand NRCA.

1.3.5 Other Participants

1.3.5.1. Policy Authority

Policy Authority (PA) is a committee setup by the Electronic Transactions Development Agency (Public Organization). The members of PA are luminaries on PKI. The duty of PA is to decide that a set of requirements for certificate issuance and use are sufficient for a given application. The PA has roles and responsibilities as follows:

1. Establish certificate policy and certification practice statement of Thailand NRCA and other certification authorities under the Thailand NRCA trust model;
2. Arrange for a review of certificate policy and certification practice statement of Thailand NRCA and other certification authorities under the Thailand NRCA trust model on a regular basis; and
3. Promote trust relationship of Thailand NRCA with other domestic or overseas certification authorities.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

The usage of a certificate issued by Thailand NRCA is limited to support the following core security needs:

- certificate signing –verify the certificate of CA subscriber ;
- certificate revocation list (CRL) signing – sign and publish CRLs

1.4.2 Prohibited Certificate Uses

A certificate issued by Thailand NRCA shall be used only for the purpose as specified in Section 1.4.1, and in particular shall be used only to the extent the use is consistent with applicable laws.

1.5 Policy Administration

1.5.1 Organization Administering the Document

This document is administered by Thailand NRCA. This document is publicly available with approval from PA.

1.5.2 Contact Person

The Director of Office of Information Technology Infrastructure,
Thailand National Root Certification Authority
Electronic Transactions Development Agency (Public Organization)
The9th Tower Grand Rama9 Building (Tower B) Floor 21
33/4 Rama 9 Road, Huai Khwang, Bangkok 10310
Tel: (66)-2123-1234
Email: nrca@etda.or.th
Website: http://www.nrca.go.th

1.5.3 Person Determining CPS Suitability for the Policy

The PA determines the suitability and applicability of this CPS.

1.5.4 CPS Approval Procedures

The CPS approval procedures are as follows:

1. Thailand NRCA proposes CPS changes and submits to PA.
   1.1. In case PA has no further comments, PA approves CPS.
   1.2. In case PA has comments, PA returns CPS to Thailand NRCA for proper modification or correction before resubmission.
2. Thailand NRCA announces and publishes CPS to the channel as listed in Section 2.2.

1.5.5 CP Review and update Procedures

NRCA shall review latest of Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates from https://cabforum.org/baseline-requirements-documents/ or http://www.webtrust.org/ at least quarterly for the purpose of develop, implement, enforce and annually update a Certificate Policy and Certificate Practice Statement.

1.6 Definitions and Acronyms

1.6.1 Definitions

See Table 1 for a list of definitions.

Term	Definition
Certificate	A form of electronic documents used for verifying the relationship between entities and public key. A certificate is issued in compliance with ITU-T Recommendation X.509 (11/08): Information technology - Open systems interconnection - The Directory: Public-key and attribute certificate frameworks and ISO/IEC 9594-8:2008 Information technology -- Open Systems Interconnection -- The Directory: Public-key and attribute certificate frameworks.
Certificate Policy (CP)	The document, which is entitled “Thailand National Root Certification Authority Certificate Policy”, describes the principal statement and applications of certificates.
Certificate Repository	Source for storage and publication of certificates and certificate revocation lists.
Certificate Revocation	A certificate may be revoked prior to its expiration date. Once revoked, it can no longer be used.
Certification Authority (CA)	An entity authorized to issue, manage, revoke, and renew certificates.
Certification Practice Statement (CPS)	The document, which is entitled “Thailand National Root Certification Authority Certification Practice Statement”, describes the procedures and scope of the certification authority, duties and obligations of the parties that acts in reliance of a certificate.
Cryptographic Module	Specialized equipment used to maintain, manage and operate the key pair.
Digital Signature	A Digital Signature is a mathematical scheme for demonstrating the authenticity and integrity of a digital message or document.
Directory Service	A storage for publication of certificates and certificate revocation lists following the X.500 Standard or LDAP.
Entity	Individual, Server, Operating Unit / Site, or any Device that is under the control of the individual.
Key Pair	A Key Pair refers to two separate keys of the asymmetric cryptographic system, one of which is secret (Private Key) and another is public (Public Key). The two parts of the key pair are mathematically linked in the ways

Term	Definition
	that one key locks or encrypts the plaintext, and the other unlocks or decrypts the cipher text. Neither key can perform both functions by itself. The Key Pair can be used to authenticate the digital signature as well as maintain confidentiality of information.
OCSP (Online Certificate Status Protocol)	A protocol used for verifying status of a certificate.
Private Key	The key used to create a digital signature and can be used to decrypt the message that is encrypted with its pair of public key, to obtain the original message.
Public Key	The key used to verify a digital signature to ensure the integrity of electronic message and also to encrypt message to maintain its confidentiality.

Table 1: Terms and Definitions

1.6.2 Acronyms

Acronym	Term
CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DN	Distinguished Name
Thailand NRCA	Thailand National Root Certification Authority
PA	Policy Authority
PIN	Personal Identification Number
PKI	Public Key Infrastructure
RA	Registration Authority
ETDA	Electronic Transactions Development Agency (Public Organization)

Table 2: Acronyms

2. Publication and Repository Responsibilities

2.1 Repositories

Thailand NRCA posts all issued certificates in a publicly accessible website at the URL http://www.nrca.go.th. Thailand NRCA has implemented access controls to prevent unauthorized modification or deletion of information.

2.2 Publication of Certification Information

Thailand NRCA publishes certification information through the channel

1. On the web : www.nrca.go.th
2. By email to nrca@etda.or.th
3. By Telephone : Tel. (66)-2123-1234

2.3 Time or Frequency of Publication

- Publication of certificates and Certificate Revocation Lists is made within 24 hours after the update.
- Thailand NRCA CPS is published within one day after the approval of update.

2.4 Access Controls on Repositories

- Thailand NRCA has implemented physical access control as well as network security measures to authenticate and restrict modification or deletion to the repository. The adding, deleting, or modifying repository entries can be performed only by authorized personnel of Thailand NRCA.
- Thailand NRCA website is used as repositories for Subscribers and Relying Parties to access the publication documents.

3. Identification and Authentication

3.1 Naming

3.1.1 Types of Names

Thailand NRCA Certificates contain a Distinguished Name (DN) in the Issuer and Subject fields, following the X.501 Information technology – Open Systems Interconnection – The Directory: Models. The Distinguished Names consist of the components specified in Table 4 below.

Attribute Name	Value
Country (C) =	TH
Organization (O) =	Electronic Transactions Development Agency (Public Organization) or <organization name>
Common Name (CN) =	Thailand National Root Certification Authority - G1 or <certification authority name>

Table 3: Distinguished Name Attributes in certificates

3.1.2 Need for Names to be Meaningful

The names contained in a certificate must be in English with commonly understood semantics permitting the determination of the identity of the individual or organization that is the Subject of the certificate, for example, through the verification of Jurisdiction of Incorporation and/or Certificate of Registration issued by the Department of Business Development, Ministry of Commerce.

3.1.3 Anonymity or Pseudonymity of Subscribers

Thailand NRCA does not issue anonymous or pseudonymous certificates.

3.1.4 Rules for Interpreting Various Name Forms

Rules for interpreting distinguished name forms follow the X.501 standard. Rules for interpreting e-mail addresses follow the RFC 2822.

3.1.5 Uniqueness of Names

The distinguished names of CA subscriber must be unique within the domain of Thailand NRCA.

3.1.6 Recognition, Authentication, and Role of Trademarks

Thailand NRCA reserves no liability to any certificate applicant on the usage of Distinguished Names appearing in a certificate. The right to use the name is the responsibility of the applicant and must be in accordance to the relevant laws, regulations, legal obligations or announcements.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

Thailand NRCA requires that an authorized representative of a juristic person submits an application form on behalf of the CA Subscriber and a Certificate Signing Request (CSR) that is signed by the private key of the CA Subscriber. Upon receipt of the CSR, Thailand NRCA will verify that the CA Subscriber is in possession of the corresponding private key by checking the digital signature on the CSR structure containing the public key material. Thailand NRCA will not have possession of the CA Subscriber's private keys.

3.2.2 Authentication of Organization Identity

CA Subscribers will submit their applications for certificates with the its name, business address in Thailand, and the Certificate of Corporate Registration of the CA issued by the Department of Business Development, Ministry of Commerce. Thailand NRCA verifies the information, in addition to the authenticity of the requesting representative and the representative's authorization to act in the name of the CA.

3.2.3 Authentication of Individual Identity

Thailand NRCA will only issue certificate which is not applicable for individual entity.

3.2.4 Non-verified Subscriber Information

All CA Subscriber's information contained in a certificate is verified.

3.2.5 Validation of Authority

Registration Authority is responsible for verifying and authenticating an authorized representative of a juristic person by checking the following documents

- Authorized Representative Appointment Letter from the relevant juristic person or other document of the same kind, corporate sealed and signed by the authorized representative of the juristic person, as specified under the Certificate of Corporate Registration issued by the

Department of Business Development, Ministry of Commerce, with a certified true copy of identification card or passport of the authorized director of such juristic person.

- A certified true copy of identification card or passport of the authorized representative of the juristic person. RA verifies and endorses the integrity of documents.

3.2.6 Criteria for Interoperation

PA promotes interoperation between CAs issuing certificates under Thailand NRCA trust model and other CAs which may or may not issue certificates under Thailand NRCA trust model (for example, overseas CA(s)). Thailand NRCA will interoperate with other Certification Authorities after signing the agreement or Memorandum of Understanding (MOU).

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and Authentication for Routine Re-key

Identification and authentication procedures are specified in Section 3.2.

3.3.2 Identification and Authentication for Re-key after Revocation

Identification and authentication procedures are specified in Section 3.2.

3.4 Identification and Authentication for Revocation Request

Identification and authentication procedures are specified in Section 3.2.

4. Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

Organization who wishes to operate a CA in Thailand may complete and submit an application for certificates to Thailand NRCA.

4.1.2 Enrollment Process and Responsibilities

CA Subscribers must complete an application and submit it to Thailand NRCA. By submitting a certificate application, the CA Subscriber authorizes the publication of the certificate to any other person or in the Thailand NRCA repository and thus accepts the certificate to be issued to the CA Subscriber.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

Thailand NRCA, or through its Registration Authority, is responsible for verifying and authenticating an authorized representative of a juristic person who submits the application form as specified in Section 3.2 and 3.3. The documentation required for proving the identity of the CA Subscriber organization and Authorized Representative(s) are in Section 3.2.5

If the verification proves invalid, Thailand NRCA, or through its Registration Authority, will send a rejection notice with reasons.

4.2.2 Approval or Rejection of Certificate Applications

Any certificate application that is received by Thailand NRCA for which the identity and authorization of the applicant has been validated, will be duly processed. However, Thailand NRCA will reject any application for which such validation cannot be completed.
RA will coordinate with Thailand NRCA during the process of approval or rejection of certificate applications and notifies the results to subscribers.

4.2.3 Time to Process Certificate Applications

CA Certificate applications will be processed within 30 business days, counting from the date that RA endorses the receipt of a CA certification application, to complete the processing of the application.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

Following the identity verification process, Thailand NRCA will notify the CA Subscriber the approval of application. Hence, the certificate issuance process is as follows:

1) CA Subscriber generates a key pair on its own device and a Certificate Signing Request (CSR) that conforms to PKCS # 10: Certificate Request Syntax Standard. The CSR contains the identity of CA Subscriber organization and the public key. The private key must be secured in the hardware security module.
2) Upon receipt of the CSR, Thailand NRCA will verify that the applicant is in possession of the corresponding Private Key by checking the digital signature on the CSR structure containing the public key material and CAO must verify and ensure that information in CSR must conform in

Section 6. If not conform in Section 6 CAO should reject.Thailand NRCA will not have possession of the applicants' Private Keys:

3) Upon verifying the applicant's possession of its Private Key, Thailand NRCA will generate the certificate in which the applicant's public key will be included;
4) The certificate will be delivered to the authorized representative in a secure manner such as by hand or by registered mail;
5) Upon Thailand NRCA acknowledgement of certificate acceptance by the authorized representative, the issued certificate will be published in the Thailand NRCA Repository together with its thumbprint for verifying the Subordinate CA authenticity on Thailand NRCA website;
6) Applicants can either verify the information on the certificate by browsing the certificate file or through Thailand NRCA Repository. Applicants should notify Thailand NRCA immediately of any incorrect information of the certificate.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

Thailand NRCA, or via RA, will notify the CA Subscriber the creation of a certificate and make the certificate available to the CA Subscribers.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

Upon the receipt of a certificate, the CA Subscriber must verify the information contained in the certificate and determine whether to accept or reject the certificate. The CA Subscriber may notify Thailand NRCA if it accepts the certificate or rejects the certificate for some reasons.

If the CA Subscriber fails to notify Thailand NRCA the rejection of the issued certificate within ten business days, the certificate will be considered as accepted.

4.4.2 Publication of the Certificate by the CA

Thailand NRCA will publish the issued certificates to Publication Channel of Certification Information within one business day after being notified by the CA Subscriber.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

Thailand NRCA will notify the PA whenever a certificate is issued to a CA.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

CA Subscriber can use the Private Key corresponding to the Public Key in the certificate, which issued by Thailand NRCA, in order to issue subscriber certificates signing with its digital signature to other subscribers or sign the certificate revocation list in relation to those subscriber certificates. Subscriber certificates shall be used lawfully in accordance with the CP, CPS and Terms of Service of Thailand NRCA.

4.5.2 Relying Party Public Key and Certificate Usage

Before any act of reliance, Relying Parties shall assess the certificate as follows:

- The accuracy of the digital signature in the CA Subscriber's certificate and its hierarchy (e.g.: path validation).
- The validity period of the certificates of CA subscriber, e.g.: the certificates should not expire by the time of use.
- The status of the certificate of Thailand NRCA, CA subscriber and other parents in every level of the hierarchy involved (if applicable) , e.g.: the certificate should not be revoked or suspended.
- Certificate usage shall be in accordance with Section 1.4.

4.6 Certificate Renewal

Thailand NRCA issues certificates to CAs operating under Thailand NRCA Certificate Policy and located in Thailand. The validity period of Thailand NRCA certificate is 23 years and that for all subordinate CAs are not more than 20 years. However, the PA may review on the proper validity period of such certificates. This is due to the fact that the current specification is determined with technical limitations related to the UTC Time, the certificate issued by Thailand NRCA will last no longer than the year 2580 (AD 2037).

4.6.1 Circumstance for Certificate Renewal

Not Applicable.

4.6.2 Who May Request Renewal

Not Applicable.

4.6.3 Processing Certificate Renewal Requests

Not Applicable.

4.6.4 Notification of New Certificate Issuance to Subscriber

Not Applicable.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Not Applicable.

4.6.6 Publication of the Renewal Certificate by the CA

Not Applicable.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

Not Applicable.

4.7 Certificate Re-key

Re-keying a certificate consists of creating new certificates with a different public key (and serial number) while retaining the remaining contents of the old certificate that describe the subject. The new certificate may be assigned a different validity period, key identifiers, specify a different CRL distribution point, and/or be signed with a different key. Re-key of a certificate does not require a change to the subject name and does not violate the requirement for name uniqueness. The old certificate may or may not be revoked, but must not be further re-keyed, renewed, or modified.

4.7.1 Circumstance for Certificate Re-key

Thailand NRCA requires its CA Subscribers to re-key the certificate in the following cases:

- CA Subscriber's certificate has less than 5 years before expiration or has already expired.
- CA Subscriber's certificate has been revoked.
- CA Subscriber needs to modify information in the certificate.

4.7.2 Who May Request Certification of a New Public Key

Only the CA Subscriber may request a new certificate.

4.7.3 Processing Certificate Re-keying Requests

CA Subscribers must follow the procedures of certificate re-keying requests as specified in Section 4.1.2.

4.7.4 Notification of New Certificate Issuance to Subscriber

Thailand NRCA notifies the result of new certificate issuance to its CA Subscriber according to the procedures specified in Section 4.3.2.

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

After CA Subscribers receive re-keyed certificate, they must follow the procedure in Section 4.4.1 to accept the re-keyed certificate.

4.7.6 Publication of the Re-keyed Certificate by the CA

Thailand NRCA publishes the re-keyed according to the procedure in Section 4.4.2.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

Thailand NRCA notifies the result of certificate issuance to other entities according to the procedure in Section 4.4.3.

4.8 Certificate Modification

Modifying a certificate means creating a new certificate that has the same or a different key and a different serial number, and that differs in one or more other fields from the old certificate. The old certificate may or may not be revoked, but must not be further re-keyed, renewed, or modified.

4.8.1 Circumstance for Certificate Modification

Since the interpretation of modifying certificate contents are sometimes complex, Thailand NRCA does not offer certificate modification. If a circumstance for certificate modification is deemed to arise, re-certification will be followed, that means the initial registration process as described in section 3.2 will be gone through again. The new certificate shall have a different subject public key.

4.8.2 Who May Request Certificate Modification

Not Applicable.

4.8.3 Processing Certificate Modification Requests

Not Applicable.

4.8.4 Notification of New Certificate Issuance to Subscriber

Not Applicable.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

Not Applicable.

4.8.6 Publication of the Modified Certificate by the CA

Not Applicable.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

Not Applicable.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

Thailand NRCA shall revoke a CA subscriber's certificate in the following circumstances:

- CA subscriber wants to discontinue the use of the certificate.
- CA subscriber does not follow Thailand NRCA's CP, and/or the CA Subscriber's own CPS.
- CA subscriber has violated relevant laws, regulations, legal obligations or announcements.
- CA subscriber's private key or CA's private key is lost or compromised.
- CA subscriber's information or CA's information in the certificate is no longer valid.
- CA subscriber experiences incident that is believed to significantly impact trustworthiness of the certificate.
- The Subscriber notifies the CA that the original certificate request was not authorized and does not retroactively grant authorization
- The CA obtains evidence that the Subscriber's Private Key (corresponding to the Public Key in the Certificate) has suffered a Key Compromise, or that the Certificate has otherwise been misused
- The CA is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber or Terms of Use Agreement
- The CA is made aware of any circumstance indicating that use of a Fully-Qualified Domain Name or IP address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name)
- The CA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name.
- The CA is made aware of a material change in the information contained in the Certificate.
- The CA is made aware that the Certificate was not issued in accordance with these Requirements or the CA's Certificate Policy or Certification Practice Statement
- The CA determines that any of the information appearing in the Certificate is inaccurate or misleading.

- The CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate.
- The CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the CA has made arrangements to continue maintaining the CRL/OCSP Repository.
- The CA is made aware of a possible compromise of the Private Key of the Subordinate CA used for issuing the Certificate.
- Revocation is required by the CA's Certificate Policy and/or Certification Practice Statement.

- The technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties (e.g. the CA/Browser Forum might determine that a deprecated cryptographic/signature algorithm or key size presents an unacceptable risk and that such Certificates should be revoked and replaced by CAs within a given period of time)

4.9.2 Who Can Request Revocation

- Any subscriber may make a request to revoke the certificate for which the subscriber is responsible.
- CA Subscriber may make a request to revoke its own certificate.
- CA Subscriber may also revoke any issued certificate whenever it knows or reasonably suspects that the circumstances as specified in section 4.9.1 occurred.
- Registration Authority (RA) may also make a request to revoke a certificate for which a subscriber is responsible whenever it knows or reasonably suspects that the circumstances as specified in section 4.9.1 occurred.
- Court order

4.9.3 Procedure for Revocation Request

CA that issues certificates under this CP shall provide the procedure that requester can request for revocation 24x7. Subscriber requesting revocation is required to follow the procedures such as:

1) CA Subscriber submits the revocation request and related documents to Thailand NRCA, or via a RA of Thailand NRCA, providing that the information is genuine, correct and complete.
2) Thailand NRCA verifies and endorses the revocation requests and related documents.
3) RA is responsible for verifying and authenticating an authorized representative of a juristic person by following the procedures as specified in Section 3.2.
4) Thailand NRCA, if necessary with the assistance of a RA, will approve and process the revocation request.

5) Thailand NRCA, if necessary with the assistance of a RA, will inform the revocation result to the CA Subscriber and PA.

4.9.4 Revocation Request Grace Period

There is no grace period for revocation under this CPS.

4.9.5 Time within Which CA Must Process the Revocation Request

Thailand NRCA shall revoke certificates as quickly as practical, or within one business day after the revocation request is endorsed.

4.9.6 Revocation Checking Requirement for Relying Parties

Relying Parties are responsible for checking the validity of each certificate in the certificate path, including checks for certificate validity, issuer-to-subject name chaining, certificate policy and key usage constraints, and the status of the certificate through the Certificate Revocation List (CRL).

4.9.7 CRL Issuance Frequency

Thailand NRCA will issue a CRL within the following circumstances:

- Issue a CRL whenever a certificate is revoked.
- Issue a CRL for certificates every six months whether or not the CRL has any changes.

4.9.8 Maximum Latency for CRLs

Thailand NRCA will publish a CRL within one hour after generation.

4.9.9 On-line Revocation/Status Checking Availability

On-line status checking is provided by Thailand NRCA, but may be provided by the CA Subscriber for certificate issued by them. Where on-line status checking is supported, status information is updated and available to relying parties within 2 hours of CRL publication.

4.9.10 On-line Revocation Checking Requirements

Relying Parties may optionally check the status of subscriber certificates through the CA Subscriber's Online Certificate Status Protocol (OCSP) service, if provided. Client software using on-line status checking need not obtain or process CRLs.

4.9.11 Other Forms of Revocation Advertisements Available

Not Applicable.

4.9.12 Special Requirements Regarding Key Compromise

Thailand NRCA, CA Subscriber and subscribers must notify Relying Parties as soon as practical regarding its key compromise.

4.9.13 Circumstances for Suspension

Under no circumstances a certificate would be suspended. If a certificate is no longer considered as valid, it will be revoked.

4.9.14 Who Can Request Suspension

Not Applicable.

4.9.15 Procedure for Suspension Request

Not Applicable.

4.9.16 Limits on Suspension Period

Not Applicable.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

The status of certificates is available through the Thailand NRCA's website and LDAP server.

4.10.2 Service Availability

Thailand NRCA has implemented backup systems for providing certificate status services and put the best efforts to make such services available 24x7.

4.10.3 Optional Features

Not Applicable.

4.11 End of Subscription

CA Subscriber may end a subscription by allowing its certificate to expire or revoking its certificate without requesting a new certificate.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

Not Applicable.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Private Keys of a CA that issues certificates under the Thailand NRCA are never escrowed.

5. Facility, Management, and Operational Controls

5.1 Physical Controls

5.1.1 Site Location and Construction

The systems providing Thailand NRCA services are located at two secure facilities i.e. the main site in Bangkok and the disaster recovery site in a geographic location reasonably apart from the main site. Both secure facilities are equipped with physical access controls as follows:

- Four layers of physical access controls
- Two-factor authentication for accessing the server rooms
- CCTVs (Closed Circuit Televisions) record the activity in the server room at all times
- Smoke detector and fire extinguisher (using electronic equipment safe agent) systems

The server rooms are accessible by the Thailand NRCA officers only. If a non-Thailand NRCA officers require to access the room, authorization from Thailand NRCA must be provided in order to allow that person to enter the server room. At all time, such a person must be accompanied by the Thailand NRCA officer.

Certificate issuing servers and Cryptographic Module are stored in a separate rack where physically accessing to such systems requires a user to perform a two-factor authentication.

5.1.2 Physical Access

Accessing the certificate issuance system is allowed only to Thailand NRCA responsible officers. In case that a third party who need to access the service area of Thailand NRCA, prior authorization must be obtained. All visits to the Thailand NRCA premise must be recorded in the access log. At all time, third parties must be accompanied by the Thailand NRCA officer during the whole visit.

Certificate issuing servers and Cryptographic Module are stored in a secure rack where physical access to such systems requires dual-control and two-factor authentication.

5.1.3 Power and Air Conditioning

- Both secure facilities are equipped with power generators and Uninterrupted Power Supplies (UPS) sufficient for 6-hours operation in the absence of commercial power, in order to maintain availability and avoid denial of service.
- The air-conditioning systems for both secure facilities maintain temperature and the humidity of the server rooms to the appropriate level.

5.1.4 Water Exposures

The secure facilities are equipped with the water sensors under the raised floor.

5.1.5 Fire Prevention and Protection

The certificate issuing area is equipped with a smoke detector where the fire extinguisher will be automatically activated when the smoke is detected.

The certificate issuing area is equipped with fire extinguishing system that operates quickly and effectively without causing damage to electrical equipment.

5.1.6 Media Storage

All magnetic media holding back ups of critical system data or any other sensitive information are protected from water, fire, or other environmental hazards, and protective measures are in place to deter, detect, and prevent the unauthorized use of, access to, or disclosure of such media.

5.1.7 Waste Disposal

Thailand NRCA has implemented procedures for the disposal of waste (paper, media, or any other waste) to prevent the unauthorized use of, access to, or disclosure of waste containing Confidential/Private Information.

5.1.8 Off-site Backup

Backup media is stored at the secure disaster recovery facility.

5.2 Procedural Controls

5.2.1 Trusted Roles

A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. It is essential that the people selected to fill these roles shall be held accountable to perform designated actions correctly or the integrity of the CA is weakened. The functions performed in these roles form the basis of trust in the CA. Thailand NRCA takes two approaches to increase the likelihood that these roles can be successfully carried out:

- The first approach is to minimize the number of trusted roles and ensure that the people filling those roles are trustworthy and properly trained.
- The second is to enforce the concept of least privilege and distribute the functions of the roles among several people, so that any malicious activity requires collusion.

Trusted role operations include:

- The validation, authentication, and handling of information in Certificate Applications
- The acceptance, rejection, or other processing of Certificate Applications, revocation requests renewal requests, or enrollment information
- The issuance, or revocation of Certificates, including personnel having access to restricted portions of its repository
- Access to safe combinations and/or keys to security containers that contain materials supporting production services
- Access to hardware security modules (HSMs), their associated keying material, and the secret share splits of the PINS that protect access to the HSMs
- Providing enterprise customer support
- Access to any source code for the digital certificate applications or systems
- Access to restricted portions of the certificate repository
- The ability to grant physical and/or logical access to the CA equipment
- The ability to administer the background investigation policy processes

Multiple people may hold the same trusted role, with collective privileges sufficient to fill the role. Other trusted roles may be defined in other documents, which describe or impose requirements on the CA operation.

Thailand NRCA defines trusted roles and rights as follows:

- Policy Authority (PA)
- Certification Authority Manager (CAM)
- Certification Authority Officer (CAO)
- Registration Authority (RA)
- Security Officer (SO)
- System Administrator (SA)
- Network Administrator (NA)
- Software Developer (SD)
- Internal Auditor (IA)

Position	Trusted Roles	Rights
Committee	Policy Authority: PA	Issue and approve the policy and the CP/CPS of the Thailand NRCA and other certification authorities located in Thailand
The Director of Office of Information	Certification Authority	● Access to the certificate issuing facilities.

Technology Infrastructure	Manager: CAM	• Access to the Cryptographic Module and give authorization to who can access the Cryptographic Module.
Secretary of Office of Information Technology Infrastructure Managers of Office of Information Technology Infrastructure	Registration Authority: RA Security Officer: SO	• Access to the list of CA Subscribers. • Access to the personal information of CA subscribers. • Access to audit logs • Access to the certificate issuing and supporting facilities. • Hold all privilege account passwords for all systems.
Managers of Office of Information Technology Infrastructure	Certification Authority Officer: CAO	• Access to the certificate issuing facilities • Hold the multi-person control token for managing the Cryptographic Module.
Engineers of Office of Information Technology Infrastructure	System Administrator: SA Network Administrator: NA	• Access to the facilities in relation to certificate issuance; • Access to the configuration of equipment such as network, firewall, antivirus, backup, etc.;
Engineers of Office of Information Technology Infrastructure	Software Developer: SD (If applicable)	• Access to the facilities in relation to software development
Independent third-party	Internal Auditor: IA	• Access to information in relation with audit matters on a need to know basis

Table 4 List of the trusted roles and their rights

5.2.2 Number of Persons Required per Task

Where multi-party control is required, all participants shall hold a trusted role. Multi-party control shall not be achieved using personnel that serve in a Security Auditor role with the exception of audit functions. The following tasks shall require two or more persons:

- Generation, activation, and backup of CA keys
- Performance of CA administration or maintenance tasks
- Archiving or deleting CA audit logs. At least one of the participants shall serve in a Security Auditor role
- Physical access to CA equipment

- Access to any copy of the CA cryptographic module
- Processing of third party key recovery requests

For the tasks that require access to the Thailand NRCA's private key, issuing a certificate, and revoking a certificate, such tasks require at least two authorized officers from the trusted roles.

5.2.3 Identification and Authentication for Each Role

Thailand NRCA and its RAs have confirmed the identity and authorization of all personnel seeking to become Trusted before such personnel are:

- issued with their access devices and granted access to the required facilities;
- given electronic credentials to access and perform specific functions on Information Systems and Thailand NRCA or RA systems.

Individuals holding trusted roles identify themselves and be authenticated by the Thailand NRCA and RA before being permitted to perform any actions set forth above for that role or identity. Thailand NRCA Operations Staff and RA Staff have authenticated using a credential that is distinct from any credential they use to perform non-trusted role functions. This credential are generated and stored in a system that is protected to the same level as the CA system.

Thailand NRCA and RA equipment are under strong authenticated access control for remote access using multi-factor authentication. Thailand NRCA and RA equipment require, at a minimum, authenticated access control (e.g., strong passwords) for local multi-party access.

Individuals holding trusted roles will be appointed to the trusted role by an appropriate approving authority. The approvals are recorded in a secure and auditable fashion. Individuals holding trusted roles accept the responsibilities of the trusted role, and this acceptance is recorded in a secure and auditable fashion. Identity proofing of RA will be performed by a member of the CA Operations Staff. Users must authenticate themselves to all aspects of the network (servers, operating systems, applications, databases, processes, and so on) before they can access that resource.

5.2.4 Roles Requiring Separation of Duties

Individuals serving as Security Auditors shall not perform or hold any other trusted role.

An individual that holds any Thailand NRCA Operations Staff role shall not be an RA except that Thailand NRCA Operations Staff may perform RA functions when issuing certificates or issuing certificates to RA.

Under no circumstances shall Thailand NRCA be audited for compliance by any subsidiary, parent, or sibling company of its corporate holdings.

Only an individual serving in a Security Auditor role may perform internal auditing functions, with the exception of those security audit functions (e.g., configuring, archiving, deleting) that require multi-person control.

An individual that performs any trusted role shall only have one identity when accessing Thailand NRCA equipment.

The following roles must be performed by trusted officers:

- Verification and validation of forms such as the certificate application forms and the certificate revocation form.
- CA Certificate issuance and revocation.
- Access to the Thailand NRCA's private key.

5.3 Personnel Controls

5.3.1 Qualifications, Experience and Clearance Requirements

Thailand NRCA personnel must be examined with their qualifications in terms of the requisite background, experience in order to ensure their prospective job responsibilities, competency and satisfaction. Thailand NRCA conducts investigations of personnel who serve in trusted roles (prior to their employment and periodically thereafter as necessary) to verify such employee's trustworthiness and competence in accordance with the requirements of this CPS and Thailand NRCA's personnel policies. Personnel who fail an initial or periodic investigation are not permitted to serve or to continue to serve in a trusted role.

5.3.2 Background Check Procedures

Prior to commencement of employment, the Human Resource Department of ETDA conducts the following background checks:

- Identification card
- House registration
- Certificate of the highest education
- Criminal records
- Professional certificate (if any)
- Confirmation letter of previous employment

Thailand NRCA may also exercise other measurements for background check. If the provided information is found to be false, or if the education/professional background is found unmatched, or if the person has certain criminal convictions, that person shall not be considered to work with Thailand NRCA.

5.3.3 Training Requirements

Thailand NRCA provides its officers with appropriate training as well as the requisite on-the-job training needed to perform their job responsibilities related to CA operations with competency and satisfaction. The training programs include the following as relevant:

- Basic cryptography and Public Key Infrastructure (PKI) concepts

- Information Security Awareness
- Use and operation of deployed hardware and software related to CA operations
- Security Risk Management
- Disaster recovery and business continuity procedures

5.3.4 Retraining Frequency and Requirements

Thailand NRCA provides its officers with appropriate training at least once a year on the topics related to Information Security Awareness. Additional training may be considered if there is a change in hardware and software related to CA operations.

5.3.5 Job Rotation Frequency and Sequence

Thailand NRCA requires its officers rotating job role every two years.

5.3.6 Sanction for Unauthorized Actions

Appropriate disciplinary actions are taken for unauthorized actions or other violations of Thailand NRCA policies and procedures. Disciplinary actions are commensurate with the frequency and severity of the unauthorized actions and may include measures up to and including termination.

5.3.7 Independent Contractor Requirements

In case that independent contractors or consultants is employed and is obliged to pass the background check procedures specified in Section 0. Any such contractor or consultant are only permitted to access to Thailand NRCA's secure facilities if they are escorted and directly supervised by trusted Thailand NRCA officers at all times.

For system maintenance purposes, operating staffs must present their employee identification card to Trusted Persons of Thailand NRCA for verification and record. They are also escorted and directly supervised by trusted Thailand NRCA officers at all times.

5.3.8 Documentation Supplied to Personnel

Thailand NRCA provides its personnel the requisite documentation needed to perform their job responsibilities competently and satisfactorily.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

Thailand NRCA logs the following significant events:

- Key Life Cycle Management of Thailand NRCA, including:

- Key generation, backup, storage, recovery, archival, and destruction
- Cryptographic Module life cycle management events

- CA certificate life cycle management events, including:
  - CA Certificate Applications, rekey, and revocation
  - Approval or rejection of requests
  - Generation and issuance of certificates and CRL
- Security-related events including:
  - Successful and unsuccessful access attempts to Thailand NRCA systems
  - Security system actions performed by Thailand NRCA officers
  - Security profile changes
  - System crashes, hardware failures and other anomalies
  - Firewall and router activity
  - Thailand NRCA facility visitor entry/exit

Log entries include the following elements:

- Date and time of the entry
- Automatic journal entries
- Identity of the entity making the journal entry
- Type of entry
- Source of entry

5.4.2 Frequency of Processing Log

Audit logs are examined at least a weekly basis for security-related events and biannually for Key Life Cycle Management and CA certificate life cycle management events.

5.4.3 Retention Period for Audit Log

Audit logs are retained for at least 90 days.

5.4.4 Protection of Audit Log

Audit logs are protected with an electronic audit log system that includes mechanisms to project the log files from unauthorized actions.

5.4.5 Audit Log Backup Procedure

- Audit logs stored in an electronic audit log system are backup in two secure facilities
- Events Records follow the procedures below:
  1) Paper-based event records are converted into electronic format before being stored in the audit log system.

2) Thailand NRCA backup audit events specified in 5.4.1 in backup media.

5.4.6 Audit Collection System (Internal vs. External)

Audit data is generated and recorded at the machine that the event has occurred and at the audit log system.

5.4.7 Notification to Event-causing Subject

Not Applicable.

5.4.8 Vulnerability Assessments

Thailand NRCA assesses security vulnerability at least on a quarterly.

5.4.9 Penetration Test Assessments

Thailand NRCA assesses security Penetration Test at least on yearly.

5.5 Records Archival

5.5.1 Types of Records Archived

Thailand NRCA archives:

- Thailand NRCA systems
  - All audit data specified in 5.4.1
  - System configuration
  - Website
- Documentation supporting certificate applications
  - CA Certificates, CRLs, and expired or revoked certificates
  - Thailand NRCA CP and CPS
- Certificate lifecycle information
  - Forms such as Application Form, Revocation Request Form, Re-key Request Form, and certificate Acceptance Form
  - Required documents for application
  - Internal documents such as procedure manuals and system access approval request
  - Letters or memos used for communication between Thailand NRCA and external parties such as its subordinate CA.

5.5.2 Retention Period for Archive

Records shall be retained for at least 10 years, unless there are specific requirements (according to the Accounting Act B.E. 2543)

5.5.3 Protection of Archive

Records archival are stored in secure facilities and can be accessed only by authorized persons.

5.5.4 Archive Backup Procedure

Records archival are backed up in backup tapes on a monthly basis following the below procedures:

1) Paper-based event records are converted into electronic format before being stored and backed up.
2) Thailand NRCA backups events records specified in Section 5.5.1 in the backup media.

5.5.5 Requirements for Time Stamping of Records

Any activity performed on or to the certification systems shall be recorded with time and date information.

5.5.6 Archive Collection System (Internal or External)

Archive Collection System is internal to Thailand NRCA only.

5.5.7 Procedures to Obtain and Verify Archive Information

Procedures to obtain and verify archive information are as follows:

1) Thailand NRCA, or via its RA, submits access request to archive information to PA specifying reasons and necessity of obtaining such information as well as identifying the type of information needed.
2) PA justifies the appropriateness and necessity of the request and notifies the decision result to the requester.
3) An authorized Thailand NRCA officer obtains the archive information, defines access rights, and forwards to the requester.
4) The requester verifies the integrity of information.

5.6 Key Changeover

To minimize risk from compromise of a Thailand NRCA's private signing key, that key may be changed often. From that time on, only the new key will be used to sign subscriber certificates.

Thailand NRCA's signing keys shall have a validity period as described in section 6.3.2.

When Thailand NRCA updates its private signature key and thus generates a new public key, Thailand NRCA will notify all CAs, RAs, and subscribers that rely on the Thailand NRCA's certificate that it has been changed.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

If compromise of Thailand NRCA is suspected, an independent third-party investigation shall be performed in order to determine the nature and the degree of damage. Certificates issuance shall be stopped immediately upon detection of a compromise. If a Thailand NRCA private signing key is suspected of compromise, the procedure outlined in section 5.7.3 shall be followed. Otherwise, the scope of potential damage shall be assessed in order to determine if Thailand NRCA needs to be rebuilt, only some certificates need to be revoked, and/or the Thailand NRCA private key needs to be declared compromised.

In case that there an event that affects the security of Thailand NRCA system, the corresponding Thailand NRCA officers shall notify PA if any of the following occur:

- Suspected or detected compromise of any Thailand NRCA system or subsystem
- Physical or electronic penetration of any Thailand NRCA system or subsystem
- Successful denial of service attacks on any Thailand NRCA system or subsystem
- Any incident preventing Thailand NRCA from issuing and publishing a CRL or on-line status checking prior to the time indicated in the *nextUpdate* field in the currently published CRL, or the certificate for on-line status checking suspected or detected compromise.

5.7.2 Computing Resources, Software, and/or Data Are Corrupted

In case of software, hardware or data failure, Thailand NRCA officers will report such incidents to the upper authorities in order to make decisions and deal with the incident properly. If it is necessary, a recovery plan may be used to restore Thailand NRCA services.

5.7.3 Entity Private Key Compromise Procedures

In the case of Thailand NRCA compromise, Thailand NRCA shall notify PA and relying parties via public announcement, and any cross-certified PKIs, of the Thailand NRCA compromise so that they can revoke any cross certificates issued to the Thailand NRCA or any Subordinate CAs and notify all Subscribers and Relying Parties to remove the trusted self-signed certificate from their trust stores. Notification shall be made in an authenticated and trusted manner. Initiation of notification to PA and any cross-certified PKIs

shall be made at the earliest feasible time and shall not exceed 24 hours beyond determination of compromise or loss unless otherwise required by law enforcement. Initiation of notification to relying parties and subscribers will be made after mediations are in place to ensure continued operation of applications and services. If the cause of the compromise can be adequately addressed, and it is determined that the PKI can be securely re-established, Thailand NRCA shall then generate a new root certificate, solicit requests and issue new certificates, securely distribute the new root certificate, and re-establish any cross certificates.

In case of a subordinate CA key compromise, the subordinate CA shall notify the PA and Thailand NRCA. Thailand NRCA shall revoke that subordinate CA's certificate, and the revocation information shall be published immediately in the most expedient, authenticated, and trusted manner but within 18 hours after the notification. The compromised subordinate CA shall also investigate and report to PA and Thailand NRCA what caused the compromise or loss, and what measures have been taken to preclude recurrence. If the cause of the compromise can be adequately addressed and it is determined that the subordinate CA can be securely re-established, then the subordinate CA shall be re-established. Upon re-establishment of the subordinate CA, new subscriber certificates shall be requested and issued again.

When a certificate of the subordinate CA is revoked because of compromise, suspected compromise, or loss of the private key, a CRL shall be published at the earliest feasible time by the subordinate CA, but in no case more than 6 hours after notification.

In case of an RA compromise, Thailand NRCA will disable RA. In the case that an RA's key is compromised, Thailand NRCA will revoke it, and the revocation information shall be published within 24 hours in the most expedient, authenticated, and trusted manner. The compromise will be investigated by Thailand NRCA in order to determine the actual or potential date and scope of RA compromise. All certificates approved by that RA since the date of actual or potential RA compromise shall be revoked. In the event that the scope is indeterminate, then the CA compromise procedures as specified in above shall be followed.

5.7.4 Business Continuity Capabilities after a Disaster

Thailand NRCA has prepared a disaster recovery plan which have been tested, verified and continually updated. A full restoration of services will be done within 24 hours in case of disaster.

5.8 CA or RA Termination

If there is any circumstance to terminate the services of Thailand NRCA with the approval of PA, Thailand NRCA will notify the subordinate CAs, the subscribers and all relying parties. The action plan is as follow:

- Notify status of the service to affected users.
- Revoke all certificates.
- Long-term store information of Thailand NRCA and its subordinate CA and subscribers according to the period herein specified.
- Provide ongoing support and answer questions.
- Properly handle Thailand NRCA or its subordinate CA key pair and associated hardware.

6. Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

Cryptographic keying material used by Thailand NRCA to sign certificates, CRLs or status information are generated in FIPS 140-2 Level 3 or equivalent standard validated cryptographic modules. Multi-party control is required for Thailand NRCA key pair generation, as specified in section 6.2.2.

Thailand NRCA key pair generation created a verifiable audit trail demonstrating that the security requirements for procedures were followed. The documentation of the procedure has shown that appropriate role separation was used. An independent third party has validated the execution of the key generation procedures by witnessing the key generation, as well as by examining the signed and documented record of the key generation.

CA Subscriber key pair generation are performed by the CA subscriber. CA subscriber is required to generate the signature key pairs for the purpose of digital signature by FIPS 140 validated hardware cryptographic modules to support source authentication.

6.1.2 Private Key Delivery to Subscriber

CA Subscribers must generate the key pair by themselves. Thailand NRCA has no policy to generate a key pair for CA subscribers.

6.1.3 Public Key Delivery to Certificate Issuer

CA Subscribers are required to submit Certificate Signing Request in the form of PKCS # 10 standard with application by themselves.

6.1.4 CA Public Key Delivery to Relying Parties

Relying parties can access Thailand NRCA public key in the certificate by the published channel.

6.1.5 Key Sizes

Currently Thailand NRCA has one root certificate and this root certificate contains a public key of RSA 4096 bits key length and is signed with the corresponding private key by using SHA-512 signature algorithm. Key sizes shall be assessed by PA at least once a year or as necessary especially in an incident that is believed to significantly impact trustworthiness of Thailand NRCA.

Subordinate CAs of Thailand NRCA will also use the same signature algorithm of Thailand NRCA and a key size no larger than that of Thailand NRCA.

6.1.6 Public Key Parameters Generation and Quality Checking

Not Applicable.

6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field)

The use of a specific key is constrained by the key usage extension in the X.509 certificate. All certificates include a critical key usage extension.

Thailand NRCA allows using its key pair for digital signature verification, signing certificate to other certification providers (Certificate Signing) and certificate revocation (CRL Signing). Public key that are bound into issued certificates is used only for signing certificates and status information such as CRLs. Only Thailand NRCA shall issue certificates to CAs located in Thailand.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

Thailand NRCA uses a FIPS 140-2 Level 3 validated hardware cryptographic module for signing operations.

Subordinate CA of Thailand NRCA shall use a FIPS 140-2 Level 3 or higher validated hardware cryptographic module for signing operations.

6.2.2 Private Key (n out of m) Multi-person Control

Accessing private key of Thailand NRCA must be performed by at least two persons with Trusted Role.

6.2.3 Private Key Escrow

Thailand NRCA does not have policy to keep private key with other parties or keep its subscribers' private key.

6.2.4 Private Key Backup

Thailand NRCA's private signature key is backed up under the same multiparty control as the original signature key. More than one copy of the private signature key are stored off-site. All copies of the CA

private signature key are accounted for and protected in the same manner as the original. Thailand NRCA backup its private signature key in FIPS 140-2 Level 3 validated hardware cryptographic module.

6.2.5 Private Key Archival

Thailand NRCA private key beyond the validity period will be kept at least 10 years and stored in Cryptographic Module with FIPS 140-2 Level 3 standards.

6.2.6 Private Key Transfer into or from a Cryptographic Module

The backup of Thailand NRCA private key must perform through Cryptographic Module with FIPS 140-2 Level 3 standards. Importing and exporting process of private key requires at least two persons with Trusted Role.

6.2.7 Private Key Storage on Cryptographic Module

Thailand NRCA private key stored in a Cryptographic Module and back up the private key in another Cryptographic Module.

6.2.8 Method of Activating Private Key

Activation of Thailand NRCA's private key operations performs by authorized person and requires two-factor authentication process.

6.2.9 Method of Deactivating Private Key

After working with the private key of Thailand NRCA, all certificate authority officers must leave the system (Log Out) to prevent unauthorized access.

6.2.10 Method of Destroying Private Key

Thailand NRCA will delete the private keys from Cryptographic Module and its backup by overwriting the private key or initialize the module with zeroization function.
The event of destroying Thailand NRCA must be recorded into evidence under section 5.4.

6.2.11 Cryptographic Module Rating

Cryptographic Module Rating complies with FIPS 140-2 Level 3 standard.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

Public key is stored for long period in the certificate.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The certificate validity period and key pair associated with the certificate can be used up to the expiry date specified in the certificate. Public key can be used to verify the digital signature even if the certificate is expired but the digital signature to be verified must be created before expiry date of the certificate. For the private key, it can be used to decrypt even if certificate is expired.

The validity period of Thailand NRCA root certificate is 23 years and validity period of CA Subscriber certificate is not more than 20 years. Certificate operational periods and key pair usage periods shall be assessed by PA at least once a year or as necessary especially in an incident that is believed to significantly impact trustworthiness of Thailand NRCA.

(Due to the technical limitations on UTC Time, the certificate issued by Thailand NRCA will last no longer than the year 2580 (AD 2037)).

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

Thailand NRCA activation data, such as Personal Identification Number (PIN) and passwords for accessing the CA systems, are user-selected and protected under multi-person control by each of whom holding that activation data. Subordinate CAs use the same data generation mechanism.

6.4.2 Activation Data Protection

Data used to unlock private keys is protected from disclosure by storing in safe and allow only authorized person to access.

6.4.3 Other Aspects of Activation Data

Not Applicable.

6.5 Computer Security Controls

Thailand NRCA has implemented multi-person control access to information such as sensitive details about customer accounts and passwords. Ultimately CA-related private keys are carefully guarded, along with the machines housing such information. Security procedures are in place to prevent and detect unauthorized access, modification, malicious code or compromise of the Thailand NRCA systems such as firmware and software. Such security controls are subject to compliance assessment as specified in section 8.

6.5.1 Specific Computer Security Technical Requirements

Thailand NRCA limits the number of application installed on each computer to minimize security risks. Those applications are hardened based on the instructions provided by software manufacturer. In addition, installed applications shall be regularly reviewed for security updates to ensure that no vulnerability is exposed.

6.5.2 Computer Security Rating

Thailand NRCA applies ISO/IEC 27001 (Information Security Management System) and Trust Service Principles and Criteria for Certification Authorities Version 2.0.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

For both readymade software and in-house developed software by Thailand NRCA that are used in certificate management, they shall be checked to ensure the software is genuine and fully tested in non-production environment before deployment in production environment. Any change to Thailand NRCA systems or components must go through the Change Management Control review and approval process.

6.6.2 Security Management Controls

Thailand NRCA has procedures to monitor and control variables of the certificate system. Changes of variables are processed through security management control.

6.6.3 Life Cycle Security Controls

Not Applicable.

6.7 Network Security Controls

Thailand NRCA network equips firewall with features to investigate data transmission at application level and detect intruders or network activities that violate policy. It is to ensure that system is secure.

Normal users allow accessing the certificate services through the network via the website and directories only. For system management, certification authority officers will use dedicated network to access and management purpose. Information contains in this particular network is encrypted.

6.8 Time-stamping

The system clock will be set in the time setting device (NTP Server) which shall be accurate to within three minutes. Any recording time in the system will refer to the same time setting device.

7. Certificate, CRL and OCSP Profiles

7.1 Certificate Profile

Certificate issued by Thailand NRCA is complied with ITU-T Recommendation X.509 (11/08): Information technology - Open systems interconnection - The Directory: Public-key and attribute certificate frameworks and ISO / IEC 9594-8:2008 Information technology standard. - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks in which the certificate contains the information shown in Table 5.

Field	Value or Value Constraint
version	Version of certificate, the details are described in section 7.1.1
serialNumber	Reference number of each Certificate Authority is unique
signature	The method of digitally sign consists of Asymmetric cryptographic algorithms (Public Key Algorithm) and data digestion (Hash Function) which Certificate Authority is used to sign the certificate in form of Object Identifier (OID).
issuer	The name of the Certificate Authority in the certificate must be in the format of Distinguished Name (DN) in accordance with ISO / IEC 9594-2.
validity	Period of certificate usage is specified by the begin date (notBefore) and expiration date (notAfter)
subject	Specify the entity name of Certificate Authority as the owner of public key in the certificate
subjectPublicKeyInfo	Specify the type of public key and subject value of public key

Table 5 Fields in the Certificate

7.1.1 Version Number

Certificate issued by Thailand NRCA is in accordance with ITU-T Recommendation X.509 standard ISO / IEC 9594-8:2008 and designated to be version 3.

7.1.2 Certificate Extensions

Additional information on the certificate issued by Thailand NRCA is complied with ISO / IEC 9594-8:2008 standard, which contains at least the following:

7.1.2.1. Key Usage

This extension shall be marked as critical. Certificates shall assert the minimum required for functionality. Thailand NRCA certificate assert at least *keyCertSign* and *CRLSign*.

7.1.2.2. Certificate Policies Extension

The Thailand Root Certificate (NRCA) SHOULD NOT contain the Certificate Policies Extension. But subordinate CA may include the CA/Browser Forum reserved identifiers or an identifier (OID) defined by the CA in its Certificate Policy and/or Certification Practice Statement to indicate the Subordinate CA's compliance with these Requirements, and set Critical to True.

7.1.2.3. Subject Alternative Name

See section 3.1.

7.1.2.4. Name Constraints

The Thailand NRCA Root Certificate does not assert Name Constraints. It may be asserted in Thailand NRCA's Subordinate certificate if required.

7.1.2.5. Basic Constraints

Specify the type of certificate in the CA Field and the maximum number of Certificate Chain that is certified in a hierarchy. The certificate of Thailand NRCA's Subordinate Certificate Authority will have CA Field set to True and *pathlen* set to none.

7.1.2.6. Extended Key Usage

Thailand NRCA Root Certificate does not contain Extended Key Usage extension.

7.1.2.7. CRL Distribution Points

Specify the point where certificate revocation list can be accessed in the form of directoryName, URL.

7.1.2.8. Authority Key Identifier

Specify the related information with public key of Certificate Authority into certificate of subscribers by hashing the public key of Certificate Authority with Hash Algorithm SHA-512.

7.1.2.9. Subject Key Identifier

Specify the related information with public key by hashing the public key in the certificate with Hash Algorithm SHA-512.

7.1.2.10. Algorithm Object Identifiers

The OID of digital signature and encryption of certificate is in Table 6

Algorithm	Object Identifier
RSAEncryption	1.2.840.113549.1.1.1
SHA512withRSAEncryption	1.2.840.113549.1.1.13

SHA512	2.16.840.1.101.3.4.2.3

Table 6 Method of digital signature and encryption with Object Identifier

7.1.3 Algorithm object identifiers

7.1.4 Name Forms

The name format of Issuer and Subject are specified in the certificate as reference to the section 3.1.1.

7.1.5 Name Constraints

The Thailand NRCA Root Certificate does not assert Name Constraints. It may be asserted in Thailand NRCA's Subordinate certificate if required.

7.1.6 Certificate Policy Object Identifier

Not Applicable.

7.1.7 Usage of Policy Constraints Extension

Not Applicable.

7.1.8 Policy Qualifiers Syntax and Semantics

Not Applicable.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

Not Applicable.

7.2 CRL Profile

Thailand NRCA's certificate revocation list comply with ITU-T Recommendation X.509 standard and ISO / IEC 9594-8:2008 has following details as in Table 7.

Field	Value or Value Constraint
version	Version of the certificate revocation list will be version number 2 as provided in section 7.2.1.
signature	The method of digitally sign consists of Asymmetric cryptographic algorithms (Public Key Algorithm) and data digest (by Hash Function)

Field	Value or Value Constraint
	which Certificate Authority uses to sign the certificate in form of Object Identifier (OID).
issuer	The name of the Certificate Authority in the certificate must be in the format of Distinguished Name (DN) in accordance with ISO / IEC 9594-2.
thisUpdate	The date and time of the revocation list.
nextUpdate	Specified date and time to the next update of certificate revocation list. If necessary Thailand NRCA will issue the certificate revocation list before schedule.
revokedCertificates	A list of the serialNumber of the certificate has been revoked with specific the date and time of revocation.

Table 7 Item list in Certificate Revocation

7.2.1 Version Number(s)

The version number of certificate revocation list in accordance with the ITU-T Recommendation X.509 and ISO / IEC 9594-8:2008 will be specified the value of version to be 2.

7.2.2 CRL and CRL Entry Extensions

The information on certificate revocation lists issued by Certification Authority is complied with ISO / IEC 9594-8:2008 standard and contains at least the following:

7.2.2.1. authorityKeyIdentifier

This attribute indicates information associated with the public key of the certificate which is digitally signed by subscribers. The signing uses SHA-512 hashing algorithm of public key of Certificate Authority.

7.2.2.2. BaseCRLNumber

This attribute indicates the sequence number that Certificate Authority assigns to each revoked certificate to order the certificate revocation list.

7.2.2.3. reasonCode

This attribute indicates the Reason Code (0-9) of revoked certificate.

7.2.2.4. invalidityDate

This attribution indicates start time when using the pair of private key and the revoked certificate is insecure. It is defined in Greenwich Mean Time (GMT) format.

7.2.2.5. issuingDistributionPoint

This attribution is used to locate the certificate revocation list (Distribution Point) and indicates that the certificate revocation list is for a Certification Authority or subscribers including the reasons of revocation (Reason Code).

7.3 OCSP Profile

Not Applicable.

7.3.1 Version Number(s)

Not Applicable.

7.3.2 OCSP Extensions

Not Applicable.

8. Compliance Audit and Other Assessments

Thailand NRCA has a compliance audit mechanism in place to ensure that the requirements of its CPS are being implemented and enforced.

8.1 Compliance audit for Subordinates CA

For the Subordinate CA that is technically constrained in accordance with SSL baseline Requirements Section 9.7. CA monitors the Subordinate CA's adherence to the CA's Certificate Policy and the Subordinate CA's Certification Practices Statement and performs quarterly assessments against a randomly selected sample of at least three percent (3%) of the Certificates issued by the subordinate CA in the period beginning immediately after the last samples was taken.
For a Subordinate CA that is not technically constrained, CA verifies that Subordinate CA is audit accordance with SSL Baseline Requirements 17.1

8.2 Frequency or Circumstances of Assessment

Audit against the Trust Service Principles and Criteria for Certification Authorities Version 2.0 are performed by auditors at least once a year.

8.3 Identity/Qualifications of Assessor

Qualified auditor who demonstrates competence in the field of compliance audits, and thoroughly familiar with the CP and CPS of Thailand NRCA is employed.

8.4 Assessor's Relationship to Assessed Entity

Auditors are independent from the Thailand NRCA, or it shall be sufficiently organizationally separated from Thailand NRCA and shall provide an unbiased, independent evaluation. To insure independence and objectivity, the compliance auditor may not have served the entity in developing or maintaining Thailand NRCA's facility or certification practice statement.

8.5 Topics Covered by Assessment

The purpose of compliance audit is to verify that a CA and its RAs comply with all the requirements of the current version of this CP and the CA's CPS. The scope of assessment shall follow that in the list below.

- Trust Service Principles and Criteria for Certification Authorities Version 2

http://www.webtrust.org/homepage-documents/item54279.pdf

- WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security – Version 2.0

  http://www.webtrust.org/homepage-documents/item79806.pdf

- WebTrust Principles and Criteria - SSL Baseline with Network Security 2.0

  https://cabforum.org/baseline-requirements-documents/

8.6 Actions Taken As a Result of Deficiency

Thailand NRCA's officers must plan to improve deficiencies. (Non-conformity) based on the assessment results with explicit operating time. The plan will be submitted to auditors to ensure that sufficient security of the system is still in place.

8.7 Communication of Results

After the assessment is completed, the audit compliance report and identification of corrective measures will be sent to PA within 30 days of completion.

9. Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

Not Applicable.

9.1.2 Certificate Access Fees

Not Applicable.

9.1.3 Revocation or Status Information Access Fees

Not Applicable.

9.1.4 Fees for Other Services

Not Applicable.

9.1.5 Refund Policy

Not Applicable.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

Thailand NRCA is responsible to the damage only if the damage is caused by intention acts or gross negligence. Entities acting as relying parties, shall determine what financial limits, if any, they wish to impose for certificates used to consummate a transaction.

9.2.2 Other Assets

Not Applicable.

9.2.3 Insurance or Warranty Coverage for End-entities

Not Applicable.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

Thailand NRCA keeps following information in the scope of confidential information:

- Private key of Thailand NRCA and required information to access private key including password to access Thailand NRCA's hardware and software
- Registration application of CA Subscribers for both approved and rejected applications
- Audit Trail record
- Contingency Plan or Disaster Recovery Plan
- Security controls of Thailand NRCA's hardware and software
- Sensitive information with potential to have impact on security and reliability of Thailand NRCA's system

9.3.2 Information Not within the Scope of Confidential Information

Following information is not within the scope of confidential information:

- Certificate Practice Policy of certification authority
- Certificate uses policy
- Information inside certificate
- Certificate revocation
- Information without impact on security and reliability of Thailand NRCA's system such as articles and news

9.3.3 Responsibility to Protect Confidential Information

Thailand NRCA has security measure in place to protect confidential information.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

Thailand NRCA develop, implement and maintain a privacy policy and procedures documenting what personally identifiable information is collected, how it is stored and processed, and under what conditions the information may be disclosed.

9.4.2 Information Treated As Private

Private information in this document means related information of subscribers that is not included in the certificate or directory.

9.4.3 Information Not Deemed Private

Not deemed private information in this document means related information of subscribers that include in the certificate or directory.

9.4.4 Responsibility to Protect Private Information

Thailand NRCA has implemented security measure to protect private information.

9.4.5 Notice and Consent to Use Private Information

Thailand NRCA will use private information only if subscribers are noticed and consent to use private information in compliance with privacy policy.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

In the event of court order or administrative order, Thailand NRCA is entitled to disclose personal information required by law or officers under the law.

9.4.7 Other Information Disclosure Circumstances

None

9.5 Intellectual Property Rights

Thailand NRCA is the only owner of intellectual property rights associated with the certificate, certificate revocation information, the certificate policy and this certificate practice statement.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

Thailand NRCA assures that:

- Procedures are implemented in accordance with the CP of Thailand NRCA.
- Any certificates issued that assert the policy OIDs identified in this CPS were issued in accordance with the stipulations of this CPS.
- Certification Practice Statement (CPS) will be provided, as well as any subsequent changes, for conformance assessment.
- The CA operation is maintained in conformance to the stipulations of the CPS.
- The registration information is accepted only from approved RAs operating under an approved CPS.

- All information regarding certificate issuance and certificate revocation are processed through the procedure specified in the CPS of Thailand NRCA.

9.6.2 RA Representations and Warranties

An RA shall assure that:

- Its RA registration operation is performed in conformance to the stipulations of the approved CPS of Thailand NRCA and related regulations.
- All information contained in the certificate issued by Thailand NRCA is valid and appropriate. Evidence that due diligence was exercised in validating the information contained in the certificates is maintained.
- The obligations are imposed on subscribers in accordance with section 9.6.3, and subscribers are informed of the consequences of not complying with those obligations.

9.6.3 Subscriber Representations and Warranties

By using certificate, the CA Subscriber assure that:

- He/She accurately represents itself in all communications with the Thailand NRCA.
- The private key is properly protected at all times and inaccessible without authorization.
- Thailand NRCA is promptly notified when the private key is suspected loss or compromise.
- All information displayed in the certificate is complete and accurate.
- The certificate will be used legitimately under laws, related regulations, terms, conditions and other related service announcements of Thailand NRCA by authorized persons.

9.6.4 Relying Party Representations and Warranties

In case of relying party representations using a certificate, the relying party shall properly verify information inside the certificate before use and accepts the fault of single side verification.

9.6.5 Representations and Warranties of Other Participants

Not Applicable.

9.7 Disclaimers of Warranties

Statement under clause 9.6 cannot be terminated or forfeited unless it is amended to conform to the law.

9.8 Limitations of Liability

Thailand NRCA is responsible for any damage incurred in the event of damage caused by the use of the service stems from the willful act or gross negligence of Thailand NRCA. The response to the damage is in amount of actual damages and not more than 2 million baht per time (there may be many transactions in one time).

9.9 Indemnities

In case of the damage occurs to Thailand NRCA from the actions of subscribers or relying parties. Thailand NRCA reserves the right to claim damages.

9.10 Term and Termination

9.10.1 Term

This CPS of Thailand NRCA takes effect from the date of publication upon the approval of PA.

9.10.2 Termination

This CPS of Thailand NRCA takes effect until it is terminated.

9.10.3 Effect of Termination and Survival

This CPS remains in effect through the end of the archive period for the last certificate issued.

9.11 Individual Notices and Communications with Participants

Thailand NRCA will communicate to those participants using reliable channel as soon as possible in accordance with the importance of information.

9.12 Amendments

9.12.1 Procedure for Amendment

Amendment of CPS is subject to Thailand NRCA and it needs to be approved by PA before announcement. However, all amendments are performed pursuant to laws, regulation or other related service announcements of Thailand NRCA.

9.12.2 Notification Mechanism and Period

Thailand NRCA reserves the right to revise insignificant in this document. In case there are any significant changes, Thailand NRCA will announce on the website within seven days from the date of enforcement.

9.12.3 Circumstances under Which OID Must Be Changed

In case of the PA has the view that it is necessary to change the involved OID numbers, Thailand NRCA will change the OID and enforce the new policy using the new OID.

9.13 Dispute Resolution Provisions

9.13.1 Disputes between Issuer and subscriber

The decisions of Thailand NRCA pertaining to matters within the scope of this CPS are final. Any claims should be submitted to Thailand NRCA at the following address:

Thailand National Root Certification Authority
c/o Electronic Transactions Development Agency (Public Organization)
The9th Tower Grand Rama9 Building (Tower B) Floor 21
33/4 Rama 9 Road, Huai Khwang, Bangkok 10310

In the event of undefined, Policy Authority has jurisdiction over the dispute.

In the event of undefined, PA has jurisdiction over the dispute.

9.13.2 Disputes between Issuer and Relying Parties

Same procedure as stated in section 9.13.1. In the event of undefined, PA has jurisdiction over the dispute.

9.14 Governing Law

The laws of the Kingdom of Thailand shall govern this CPS.

9.15 Compliance with Applicable Law

Thailand NRCA are required to comply with the laws of the Kingdom of Thailand.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

This CPS shall be considered as part of the agreement between Thailand NRCA and its subscribers.

9.16.2 Assignment

Requirements of the assignment must be in accordance with laws, regulations, or announcements relating to Thailand NRCA.

9.16.3 Severability

Should it be determined that one section of this CPS is incorrect or invalid, the other sections of this CPS shall remain in effect until the CPS is updated.

9.16.4 Enforcement

Should it be determined that any section of this CPS is illegal, unenforceable, or void, then any offending words in it will be deleted to the extent necessary to make it legal and enforceable while preserving its intent.

9.16.5 Force Majeure

Provided Thailand NRCA and subordinate CAs have exercised a reasonable degree of skill and care to avoid and/or mitigate the effects of matters beyond its control, neither Thailand NRCA, the subordinate CA nor any RA is liable for the adverse effects to Subscribers or Relying Parties of any matters outside our control whatsoever, including (without limitation) the availability of the Internet, or telecommunications or other infrastructure systems or the adverse effects of the acts of God, war, military operations, national emergency, epidemic, fire, flood, earthquake, strike or riots or the negligence or deliberate wrongful conduct of other Subscribers or other third parties.

9.17 Other Provisions

Not Applicable.